

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-216766
 (43)Date of publication of application : 04.08.2000

(51)Int.Cl.

H04L 9/08
 G09C 1/00
 H04B 7/26
 H04Q 7/38

(21)Application number : 11-012227

(71)Applicant : KODO IDO TSUSHIN SECURITY GIJUTSU
 KENKYUSHO:KK

(22)Date of filing : 20.01.1999

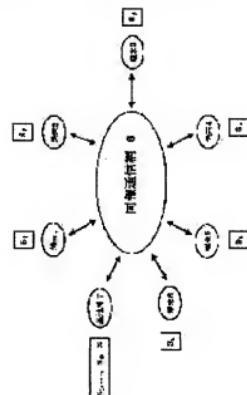
(72)Inventor : ANZAI JUN
 MATSUZAKI NATSUME
 MATSUMOTO TSUTOMU

(54) EXCLUSIVE KEY SHARING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To accelerate updating of confidential communication by allowing each terminal, capable of being specified by a base station, to hold a secret key and the secret information of a self-terminal calculated from the number of terminals and to find new secret information according to received information, when the base station conducts broadcast communication.

SOLUTION: Each terminal, (i) capable of being specified by a base station, holds a secret key S and a secret information Si satisfying a relational expression defined by a number N of terminals, and the base station holds information including an element (g) of a specified term calculated by the relational expression and secret information S1 to SN. The base station calculates preparation information C1 from the relational expression, calculates elimination information C2 from the secret information Sa of a specific terminal (a), performs broadcast communication of both the number (a) of the terminal (a) and the information C1 to all terminals, finds a shared key K with all of the terminals (i) except the terminal (a), and each terminal (i) finds the key K with the base station by using the information C1 and C2 and own confidential communication Si. The base station conducts broadcast communication to all of the terminals, finds a new element (g'), replaces it with an element (g), and each terminal (i) finds new confidential communication Si'.



LEGAL STATUS

[Date of request for examination] 02.06.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3032192

[Date of registration] 10.02.2000

[Number of appeal against examiner's decision of

[rejection]

[Date of requesting appeal against examiner's decision
of rejection]

[Date of extinction of right]

10.02.2003

(19) 日本国特許庁 (JP) (12) 公開特許公報 (A) (11) 特許出願公開番号
 特開2000-216766
 (P2000-216766A)
 (43)公開日 平成12年8月4日 (2000.8.4)

(51) Int.Cl. ¹	識別記号	F I	テマコード(参考)
H 04 L 9/08		H 04 L 9/00	6 0 1 B 5 J 1 0 4
G 09 C 1/00	6 2 0	G 09 C 1/00	6 2 0 Z 5 K 0 6 7
H 04 B 7/26	1 0 1	H 04 B 7/26	1 0 1
H 04 Q 7/38			1 0 9 S
		H 04 L 9/00	6 0 1 E
			審査請求 有 請求項の数 8 O L (全 21 頁)

(21) 出願番号	特願平11-12227	(71) 出願人	597174182
(22) 出願日	平成11年1月20日 (1999.1.20)	株式会社高度移動通信セキュリティ技術研究所	
		神奈川県横浜市港北区新横浜三丁目20番地8	
		(72) 発明者	安齋 淳
		神奈川県横浜市港北区新横浜三丁目20番地8	株式会社高度移動通信セキュリティ技術研究所内
		(74) 代理人	100099254 弁理士 役 昌明 (外1名)

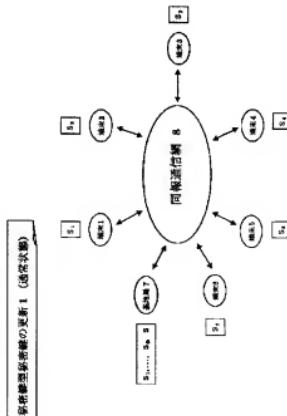
最終頁に続く

(54) 【発明の名称】 排他的鍵共有法

(57) 【要約】

【課題】 スター型通信システムにおいて、特定の端末を排除するための共通秘密鍵を、少ない通信量で高速に配送する。

【解決手段】 基地局7は秘密鍵Sを作成して秘密に保持する。秘密鍵Sを分割した秘密情報S₁を、各端末1～6に暗号通信手段を用いて秘密に配送する。準備情報C₁(= g^k mod p)と排除情報C₂(= y_b^k mod p)および特定端末番号を全端末に同報通信する。端末は、準備情報C₁と、排除情報C₂を用いて、C₁^(λ(1, λ) mod q) mod pと、C₂^(λ(5, λ) mod q) mod pとの積を計算してKを得て、基地局7との共通データとする。基地局が、零でないG F(q)の元eを任意に生成して全端末に同報通信し、新規元g' (= g^{1/e} mod p)を求めて、元gと置き換え、各端末1が、新規秘密情報S_{1'}(= S₁ × e mod q)を求める。基地局の通信量がeのみと少なく、元g以外の公開情報が変更されないので、高速に秘密情報を更新できる。



【特許請求の範囲】

【請求項1】 基地局と、前記基地局と接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、GF(p)の元をgとし、議長端末（任意の端末がなることができる）が特定できる特定端末数を1とし、前記各端末i（1≤i≤N）は、

$S = \sum \lambda(i, \Delta) \times S_i$ （和は $i \in \Delta$ について行う）
(ただし、

$S_i = S + f_i \times i \bmod q$ (f_i は零でないGF(q)の元)。

$\lambda(i, \Delta) = \prod \{L/(L-i)\}$ (積は $L \in \Delta - \{i\}$ について行う)。

△は、前記N台の端末の任意の2台からなる集合である) を満たす秘密情報 S_1 を秘密に保持しており、前記基地局は、前記 $(S, p, g, S_1, \dots, S_n)$ を保持し、

(1) 前記基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$C_1 = g^k \bmod p$

を計算し、(2) 前記基地局は、特定端末aの秘密情報 S_a から排除情報

$C_2 = g^{(\Delta)}(k \times S_a \bmod q) \bmod p$

を計算し、特定端末番号aと準備情報 C_1 と共に全端末に同報通信し、(3) 前記基地局は、前記特定端末aを除く全ての端末j ($j \neq a$)との共有鍵

$K = g^{(\Delta)}(k \times S_j \bmod q) \bmod p$

を求め、(4) 前記各端末j ($j \neq a$)は、前記準備情報 C_1 と前記排除情報 C_2 と自身の秘密情報 S_j を用いて、前記 S_j と前記 $\lambda(j, \Delta)$ の前記法 q^{Δ} 上での積を指数とする、前記 C_1 のべき乗剩余値

$C_1^{(\Delta)}(S_j \times \lambda(j, \Delta) \bmod q) \bmod p$

と、前記法 q^{Δ} 上で求めた前記 $\lambda(a, \Delta)$ を指数とする、前記 C_2 のべき乗剩余値

$C_2^{(\Delta)}(\lambda(a, \Delta) \bmod q) \bmod p$

との積

$C_1^{(\Delta)}(S_j \times \lambda(j, \Delta) \bmod q) \times C_2^{(\Delta)}(\lambda(a, \Delta) \bmod q) \bmod p$

を計算することにより、前記基地局との共有鍵Kを求め、(i) 前記基地局は、零でないGF(q)の元eを任意に生成し、前記eを全端末に同報通信し、(ii) 前記基地局は、新規元

$g' = g^{1/e} \bmod p$

を求め、前記元gと置き換え、(iii) 前記各端末iは、新規秘密情報

$S_i' = S_i \times e \bmod q$

(このとき、 $(g')^{S_i'} \bmod p = (g)^{S_i} \bmod p$ が成り立つ) を求めることを特徴とする排他的鍵共有法。

【請求項2】 相互に接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排

他的鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、GF(p)の元をgとし、議長端末（任意の端末がなることができる）が特定できる特定端末数を1とし、前記各端末i（1≤i≤N）は、

$S = \sum \lambda(i, \Delta) \times S_i$ (和は $i \in \Delta$ について行う)

(ただし、

$S_i = S + f_i \times i \bmod q$ (f_i は零でないGF(q)の元)。

$\lambda(i, \Delta) = \prod \{L/(L-i)\}$ (積は $L \in \Delta - \{i\}$ について行う)。

△は、前記N台の端末の任意の2台からなる集合である) を満たす秘密情報 S_1 を秘密に保持しており、システム管理者により管理された前記素数p、前記約数q、前記元gと、前記システム管理者により管理された全端末の公開鍵

$y = g^k \bmod p$

と、前記システム管理者により管理された公開情報

$y_1 = g^{S_1} \bmod p, y_2 = g^{S_2} \bmod p, \dots, y_n = g^{S_n} \bmod p$ を利用でき、(1) 前記議長端末は、零でないGF(q)の元kを任意に生成し、準備情報

$C_1 = g^k \bmod p$

を計算し、(2) 前記議長端末は、特定端末aの公開情報 y_a から排除情報

$C_2 = y_a^{S_1} \bmod p$

を計算し、特定端末番号aと準備情報 C_1 と共に全端末に同報通信し、(3) 前記議長端末は、共有鍵

$K = y^k \bmod p$

を求め、(4) 前記各端末j ($j \neq a$)は、 $\Delta = \{j, a\}$ として、 $\lambda(j, \Delta)$ と $\lambda(a, \Delta)$ を求め、前記準備情報 C_1 と前記排除情報 C_2 と自身の秘密情報 S_j を用いて、

$C_1^{(\Delta)}(S_j \times \lambda(j, \Delta) \bmod q) \times C_2^{(\Delta)}(\lambda(a, \Delta) \bmod q) \bmod p$

を計算することにより、前記議長端末との共有鍵Kを求め、(i) 前記システム管理者は、零でないGF(q)の元eを任意に生成し、前記eを全端末に同報通信し、

(ii) 前記システム管理者は、新規元

$g' = g^{1/e} \bmod p$

を求め、管理する前記元gと置き換え、(iii) 前記各端末iは、新規秘密情報

$S_i' = S_i \times e \bmod q$

(このとき、 $(g')^{S_i'} \bmod p = (g)^{S_i} \bmod p$ が成り立つ) を求めることを特徴とする排他的鍵共有法。

【請求項3】 基地局と、前記基地局と接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、基地局が特定できる端末数（以下、特定端末数という）を1とし、前記各端末i（1≤i≤N）は、

$S = \sum \lambda(i, \Delta) \times S_i$ (和は $i \in \Delta$ について行う)
 (ただし、
 $S_i = S + f_1 \times i \bmod q$ (f_1 は零でないGF(q)の元)、
 $\lambda(i, \Delta) = \prod \{L/(L-i)\}$ (積は $L \in \Delta - \{i\}$ について行う)、
 Δ は、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報 S_i を秘密に保持しており、前記基地局は、前記 $(S, p, g, S_1, \dots, S_n)$ を保持し、
 (1) 前記基地局は、GF(p)の元を g とし、零でないGF(q)の元を k としたとき、準備情報
 $C_1 = g^k \bmod p$
 を計算し、(2) 前記基地局は、特定端末 a の秘密情報 S_a から排除情報
 $C_2 = g^{\wedge}(k \times S_a \bmod q) \bmod p$
 を計算し、特定端末番号 a と準備情報 C_1 と共に全端末に同報通信し、(3) 前記基地局は、前記特定端末 a を除く全ての端末 j ($j \neq a$) の共有鍵
 $K = g^{\wedge}(k \times S_j \bmod q) \bmod p$
 を求め、(4) 前記各端末 j ($j \neq a$) は、前記準備情報 C_1 と前記排除情報 C_2 と自身の秘密情報 S_j を用いて、前記 S_j と前記 (j, Δ) の前記法 g^{\wedge} 上での積を指数とする、前記 C_1 のべき乗剰余値
 $C_1^{\wedge}(S_j \times \lambda(j, \Delta) \bmod q) \bmod p$
 と、前記法 g^{\wedge} 上で求めた前記 $\lambda(j, \Delta)$ を指數とする、前記 C_2 のべき乗剰余値
 $C_2^{\wedge}(\lambda(j, \Delta) \bmod q) \bmod p$
 との積
 $C_1^{\wedge}(S_j \times \lambda(j, \Delta) \bmod q) \times C_2^{\wedge}(\lambda(j, \Delta) \bmod q) \bmod p$
 を計算することにより、前記基地局との共有鍵 K を求め、(i) 前記基地局は、零でないGF(q)の元 e を任意に生成し、前記共有鍵 K を用いて暗号化した暗号化 e を全端末に同報通信し、(ii) 前記基地局は、新規元
 $g' = g^{1/e} \bmod p$
 を求め、前記元 g を置き換え、(iii) 前記各端末 j は、前記暗号化 e を前記共有鍵 K を用いて復号化し、新規秘密情報 $S_j' = S_j \times e \bmod q$
 (このとき、 $(g')^{\wedge} \bmod p = (g)^{\wedge} \bmod p$ が成立立つ)を求めることが特徴とする排他的鍵共有法。
 【請求項4】 相互に接続されたN台 (Nは2以上の整数) の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵を S とし、前記 S および前記Nより大きい素数または素数のべき数を p とし、 $(p-1)$ の約数を q とし、GF(p)の元を g とし、議長端末 (任意の端末がなることができる) が特定できる特定端末数を1とし、前記各端末 i ($1 \leq i \leq N$) は、
 $S = \sum \lambda(i, \Delta) \times S_i$ (和は $i \in \Delta$ について行う)
 (ただし、
 $S_i = S + f_1 \times i \bmod q$ (f_1 は零でないGF(q)の元))。

元)、
 $\lambda(i, \Delta) = \prod \{L/(L-i)\}$ (積は $L \in \Delta - \{i\}$ について行う)、
 Δ は、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報 S_i を秘密に保持しており、全端末の公開鍵
 $y = g^k \bmod p$
 と、公開情報
 $y_1 = g^{\wedge} \bmod p, y_2 = g^{\wedge} \bmod p, \dots, y_N = g^{\wedge} \bmod p$ を利用でき、(1) 前記議長端末は、零でないGF(q)の元 k を任意に生成し、準備情報
 $C_1 = g^k \bmod p$
 を計算し、(2) 前記議長端末は、特定端末 a の公開情報 y_a から排除情報
 $C_2 = y_a^{\wedge} \bmod p$
 を計算し、特定端末番号 a と準備情報 C_1 と共に全端末に同報通信し、(3) 前記議長端末は、共有鍵
 $K = y^k \bmod p$
 を求め、(4) 前記各端末 j ($j \neq a$) は、 $\Delta = \{j, a\}$ として、 $\lambda(j, \Delta)$ と $\lambda(a, \Delta)$ を求め、前記準備情報 C_1 と前記排除情報 C_2 と自身の秘密情報 S_j を用いて、 $C_1^{\wedge}(S_j \times \lambda(j, \Delta) \bmod q) \times C_2^{\wedge}(\lambda(a, \Delta) \bmod q) \bmod p$
 を計算することにより、前記議長端末との共有鍵 K を求め、(i) 前記議長端末は、零でないGF(p)の元 e を任意に生成し、前記共有鍵 K を用いて暗号化した暗号化 e を全端末に同報通信し、(ii) 前記議長端末は、新規元
 $g' = g^{1/e} \bmod p$
 を求め、前記元 g を置き換え、(iii) 前記各端末 j は、前記暗号化 e を前記共有鍵 K を用いて復号化し、新規秘密情報
 $S_j' = S_j \times e \bmod q$
 (このとき、 $(g')^{\wedge} \bmod p = (g)^{\wedge} \bmod p$ が成立立つ)を求めることが特徴とする排他的鍵共有法。
 【請求項5】 互相に接続されたN台 (Nは2以上の整数) の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵を S とし、前記 S および前記Nより大きい素数または素数のべき数を p とし、 $(p-1)$ の約数を q とし、GF(p)の元を g とし、議長端末 i が特定できる特定端末数を1とし、前記各端末 i ($1 \leq i \leq N$) は、
 $S = \sum \lambda(i, \Delta) \times S_i$ (和は $i \in \Delta$ について行う)
 (ただし、
 $S_i = S + f_1 \times i \bmod q$ (f_1 は零でないGF(q)の元))。
 $\lambda(i, \Delta) = \prod \{L/(L-i)\}$ (積は $L \in \Delta - \{i\}$ について行う)、
 Δ は、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報 S_i を秘密に保持しており、前記

議長端末bは、全端末の公開鍵

$$y = g^s \bmod p$$

と、公開情報

$y_1 = g^{s1} \bmod p, y_2 = g^{s2} \bmod p, \dots, y_n = g^{sn} \bmod p$ を利用でき、(1) 前記議長端末bは、零でないGF(q)の元kを任意に生成し、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2) 前記議長端末bは、特定端末aの公開情報 y_a から排除情報

$$C_2 = y_a^k \bmod p$$

を計算し、特定端末番号aと準備情報 C_1 と共に全端末に同報通信し、(3) 前記議長端末bは、共有鍵

$$K = y^k \bmod p$$

を求め、(4) 前記各端末j ($j \neq a, b$)は、 $\lambda = (j, a)$ として、 $\lambda(j, a)$ と $\lambda(a, a)$ を求め、前記準備情報 C_1 と前記排除情報 C_2 と自身の秘密情報 S_j を用いて、

$$C_1 \wedge (S_j \times \lambda(j, a) \bmod q) \times C_2 \wedge (\lambda(a, a) \bmod q) \bmod p$$

を計算することにより、共有鍵Kを求めることが特徴とする排他的鍵共有法。

【請求項6】 前記議長端末bを除く全ての端末は、前記議長端末bの公開情報

$$y_b = g^{sb} \bmod p$$

を利用して、前記議長端末bが、前記議長端末bの秘密情報 S_b を用いて、全端末に配送する特定端末番号aと準備情報 C_1 と排除情報 C_2 に、デジタル署名を付加し、前記各端末jが、前記議長端末の公開情報 y_b を用いて、署名の検証を行うことを特徴とする請求項5記載の排他的鍵共有法。

【請求項7】 上記基地局または議長端末が、上記特定端末aに対して、上記元eを配送し、上記特定端末aは、新規秘密情報

$$S_a' = S_a \times e \bmod q$$

(このとき、 $(g')^s \wedge S_a' \bmod p = (g)^s \wedge S_a \bmod p$ が成立立つ)を求めることが特徴とする請求項3、4記載の排他的鍵共有法。

【請求項8】 前記乗法演算を、任意の有限体上の梢円曲線などの曲線上の加法演算に対応させることを特徴とする請求項1～7記載の排他的鍵共有法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、基地局と複数端末からなるスター型通信システムなどにおける暗号鍵共有方法に関するもので、特に、基地局が特定した端末以外のすべての端末に共通の秘密鍵を安全に配送する鍵共有方法、および特定の端末のみに共有の秘密鍵を安全に配送する鍵共有方法に関するものである。

【0002】

【従来の技術】基地局が複数の端末を管理するスター型

通信システムにおいて、基地局と傘下の複数の端末がグループを形成し、グループで同じグループ秘密鍵を共有して同報の暗号通信を行う場合がある。この場合、グループ秘密鍵を用いて暗号化された情報は、同じ秘密鍵を保有するグループ内の端末だけが復号することができる。

【00003】ところで、このグループから特定の端末を排除したい場合が生じる。それは、例えば、グループ内のある端末が盗難にあい、その端末を用いた暗号通信の盗聴や偽情報の送信などの不正が行われるおそれがある場合などである。このとき、この秘密鍵を管理する基地局は、できるだけ速やかに、盗難にあった端末を排除してグループ秘密鍵を更新し、残りの端末だけで新たな秘密鍵を共有することが必要となる。

【00004】また、新たにグループを構成する必要が生じる場合がある。それは、グループ外の端末をグループに加入させる場合や、別のグループの端末を一つのグループにする場合などである。このとき、基地局は、できるだけ速やかに、新規グループの鍵をグループを構成する端末と共有することが必要となる。

【00005】このような目的を達成するため、本発明者は先に、以下のような効率的な排他的鍵共有法を提案した。

【0006】基地局と、基地局と接続されたN台 (Nは2以上の整数) の端末からなる同報通信が可能な通信システムにおいて、秘密鍵をSとし、SおよびNより大きい素数または素数のべき数をpとし、 $(p-1)$ の約数をqとし、基地局が特定できる端末数 (以下、特定端末数という) を1とし、各端末i ($1 \leq i \leq N$) は、 $S = \prod_{i=1}^N \lambda(i, \Lambda) \times S_i$ (和は $i \in \Lambda$ について行う) (ただし、

$$S_i = S + f_i \times i \bmod q \quad (f_i \text{は零でないGF}(q)\text{の元})$$

$\lambda(i, \Lambda) = \prod_{j \in \Lambda} \{L / (L - j)\}$ (積は $L = \Lambda - \{i\}$ について行う)

八は、N台の端末の任意の2台からなる集合) を満たす秘密情報 S_i を秘密に保持しており、基地局は、 $(S, p, g, S_1, \dots, S_N)$ を保持している。

(1) 基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$$C_1 = g^k \bmod p$$

を計算する。

(2) 基地局は、特定端末aの秘密情報 S_a から排除情報

$$C_2 = g^k (k \times S_a \bmod q) \bmod p$$

を計算し、特定端末番号aと準備情報 C_1 と共に全端末に同報通信する。

(3) 基地局は、特定端末aを除く全ての端末j ($j \neq a$)との共有鍵

$$K = g^k (k \times S_a \bmod q) \bmod p$$

を求める。

(4) 各端末 j ($j \neq a$)は、準備情報 C_1 と排除情報 C_2 と自身の秘密情報 S_j を用いて、 $S_j \times \lambda(j, \Lambda)$ の法 q 上での積を指數とする、 C_1 のべき乗剰余値

$$C_1 \hat{\wedge} (S_j \times \lambda(j, \Lambda) \bmod q) \bmod p$$

と、法 q 上で求めた $\lambda(a, \Lambda)$ を指數とする、 C_2 のべき乗剰余値

$$C_2 \hat{\wedge} (\lambda(a, \Lambda) \bmod q) \bmod p$$

との積

$$C_1 \hat{\wedge} (S_j \times \lambda(j, \Lambda) \bmod q) \times C_2 \hat{\wedge} (\lambda(a, \Lambda) \bmod q) \bmod p$$

を計算することにより、基地局との共有鍵 K を求める。

【0007】このようにして、基地局から全端末に同報通信をするだけで鍵共有ができるので、鍵共有のための業務停止期間を短くできるとともに、端末での処理が削減できるので、計算能力が高くなき端末で高速に鍵共有ができる。

【0008】

【発明が解決しようとする課題】しかし、上記の鍵共有方法では、次の3つの問題が存在する。

(1) 安全性を高めるために端末の秘密情報を定期的に更新するのが望ましいが、各端末毎に新規秘密情報を配送すると、通信量と更新が終了するまでの時間が多くなっていた。また、一般に秘密情報を更新すると公開情報の更新が必要となり、公開簿や端末がローカルに保存している公開情報の更新も行うので更新時間が多くなっていた。

(2) 前回の排他的鍵共有で排除した端末を、それ以降の全ての排他的鍵共有でも排除し続けるためには、排他的鍵共有毎に処理を必要としていた。

(3) 端末のみからなるシステムにおいて排他的鍵共有を行うには、全端末が他の全端末の公開情報を保有しているか、それが公開された公開簿が必要であった。また、誰でもが議長端末になれる方法であるので、運用上議長端末をある端末に固定しない場合に対応できなかつた。

【0009】本発明は、上記の課題を解決して、通信量と更新時間を最小に押さえて全端末の秘密情報を更新すること、排他的鍵共有毎に処理を行うことなく一度排除した端末を継続的に排除すること、各端末が全端末の公開情報を保有せず、かつ公開簿を必要ないようになると、ある端末だけが議長端末になれるようにすることを目的とする。

【0010】

【課題を解決するための手段】上記の課題を解決するために、本発明では、基地局と、基地局と接続されたN台 (Nは2以上の整数) の端末からなる同報通信が可能な通信システムの排他的鍵共有法を、秘密鍵をSとし、SおよびNより大きい素数または素数のべき数をpとし、

(p-1)の約数をqとし、基地局が特定できる端末数 (以下、特定端末数という) を1とし、各端末i (1 ≤ i ≤ N) は、

$$S_i = \sum_{j \in \Lambda} \lambda(i, j) \times S_j \quad (\text{和は } i \in \Lambda \text{ について行う})$$

(ただし、

$$S_i = S + f_1 \times i \bmod q \quad (f_1 \text{ は零でない } GF(q) \text{ の元})$$

$$\lambda(i, j) = \prod_{l \in \Lambda} \{L/(L-i)\} \quad (\text{積は } L \in \Lambda - \{i\} \text{ について行う})$$

Λ は、N台の端末の任意の2台からなる集合である) を満たす秘密情報 S_i を秘密に保持しており、基地局は、(S, p, g, S₁, ..., S_N) を保持し、(1) 基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとし、たとき、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2) 基地局は、特定端末aの秘密情報 S_a から排除情報

$$C_2 = g^{\hat{\wedge}} (k \times S_a \bmod q) \bmod p$$

を計算し、特定端末番号aと準備情報 C_1 と共に全端末に同報通信し、(3) 基地局は、特定端末aを除去全ての端末j ($j \neq a$) との共有鍵

$$K = g^{\hat{\wedge}} (k \times S_j \bmod q) \bmod p$$

を求め、(4) 各端末j ($j \neq a$)は、準備情報 C_1 と排除情報 C_2 と自身の秘密情報 S_j を用いて、 $S_j \times \lambda(j, \Lambda)$ の法 q 上での積を指數とする、 C_1 のべき乗剰余値

$$C_1 \hat{\wedge} (S_j \times \lambda(j, \Lambda) \bmod q) \bmod p$$

と、法 q 上で求めた $\lambda(a, \Lambda)$ を指數とする、 C_2 のべき乗剰余値

$$C_2 \hat{\wedge} (\lambda(a, \Lambda) \bmod q) \bmod p$$

との積

$$C_1 \hat{\wedge} (S_j \times \lambda(j, \Lambda) \bmod q) \times C_2 \hat{\wedge} (\lambda(a, \Lambda) \bmod q) \bmod p$$

を計算することにより、基地局との共有鍵 K を求める、(i) 基地局は、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、(ii) 基地局は、新規元

$$g' = g^{1/e} \bmod p$$

を求め、元gと置き換え、(iii) 各端末iは、新規秘密情報

$$S'_i = S_i \times e \bmod q$$

(このとき、 $(g')^{S'_i} \bmod p = (g)^{S_i} \bmod p$ が成立する) を求める構成とした。

【0011】このように構成したことにより、基地局の通信量がのみと少なく、システムパラメータ元g以外の公開情報が変更されないので、高速な秘密情報の更新が可能となる。

【0012】また、互に接続されたN台 (Nは2以上の整数) の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i) システム管理者は、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、(ii) システム管理者は、新規元

$$g' = g^{1/e} \bmod p$$

を求める、管理する元 g と置き換える、(iii) 各端末 i は、新規秘密情報
 $S_i' = S_i \times e \bmod q$
 を求める構成とした。

【0013】このように構成したことにより、システム管理者の通信量が e のみと少なく、システムパラメータ元 g 以外の公開情報が変更されないので、高速な秘密情報の更新が可能となる。

【0014】また、基地局と、基地局と接続されたN台(N は2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i) 基地局は、 \wedge でない $GF(q)$ の元 e を任意に生成し、共有鍵 K を用いて暗号化した暗号化 e を全端末に同報通信し、
 (ii) 基地局は、新規元

$$g' = g^{1/e} \bmod p$$

を求める、元 g と置き換える、(iii) 各端末 j は、暗号化 e を共有鍵 K を用いて復号化し、新規秘密情報
 $S_j' = S_j \times e \bmod q$
 を求める構成とした。

【0015】このように構成したことにより、排他的鍵共有で共有した共有鍵を用いて配送した乱数を用いて端末の秘密情報を更新するので、以降の排他的鍵共有で排除した端末は復帰することができない。

【0016】また、相互に接続されたN台(N は2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i) 議長端末は、 \wedge でない $GF(q)$ の元 e を任意に生成し、共有鍵 K を用いて暗号化した暗号化 e を全端末に同報通信し、(ii) 議長端末は、新規元

$$g' = g^{1/e} \bmod p$$

を求める、元 g と置き換える、(iii) 各端末 j は、暗号化 e を共有鍵 K を用いて復号化し、新規秘密情報
 $S_j' = S_j \times e \bmod q$
 を求める構成とした。

【0017】このように構成したことにより、排他的鍵共有で共有した共有鍵を用いて配送した乱数を用いて端末の秘密情報を更新するので、以降の排他的鍵共有で排除した端末は復帰することができない。

【0018】また、相互に接続されたN台(N は2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵を S とし、 S および N より大きい素数または素数のべき数を p とし、 $(p-1)$ の約数を q とし、基地局が特定できる特定端末数を1とし、各端末 i ($1 \leq i \leq N$)は、

$$S = \sum \lambda(i, \wedge) \times S_i \quad (\text{和は } i \in \wedge \text{について行う})$$

(ただし、

$$S_i = S + f_i \times i \bmod q \quad (f_i \text{は零でない } GF(q) \text{ の元})$$

$\lambda(i, \wedge) = \prod \{L / (L - i)\}$ (積は $L \in \wedge - \{i\}$ について行う)、

\wedge は、N台の端末の任意の2台からなる集合である)を満たす秘密情報 S_i を秘密に保持しており、議長端末 b は、全端末の公開鍵

$$y = g^k \bmod p$$

と、公開情報

$y_1 = g^{s_1} \bmod p, y_2 = g^{s_2} \bmod p, \dots, y_N = g^{s_N} \bmod p$ を利用でき、(1) 議長端末 b は、零でない $GF(q)$ の元 k を任意に生成し、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2) 議長端末 b は、特定端末 a の公開情報 y_a から排除情報

$$C_2 = y_a^k \bmod p$$

を計算し、特定端末番号 a と準備情報 C_1 と共に全端末に同報通信し、(3) 議長端末 b は、共有鍵

$$K = y^k \bmod p$$

を求め、(4) 各端末 j ($j \neq a, b$)は、 $\wedge = \{j, a\}$ として、 $\lambda(j, \wedge)$ と $\lambda(a, \wedge)$ を求めて、準備情報 C_1 と排除情報 C_2 と自身の秘密情報 S_j を用いて、

$$C_1 \wedge (S_j \times \lambda(j, \wedge) \bmod q) \times C_2 \wedge (\lambda(a, \wedge) \bmod q) \bmod p$$

を計算することにより、共有鍵 K を求める構成とした。

【0019】このように構成したことにより、議長端末以外の端末は他の端末の公開情報を保持する必要が無く、議長端末のみが他の端末の公開情報を利用できるでの他の端末は議長端末になれない。

【0020】

【発明の実施の形態】本発明の請求項1記載の発明は、基地局と、前記基地局と接続されたN台(N は2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵を S とし、前記 S および前記 N より大きい素数または素数のべき数を p とし、 $(p-1)$ の約数を q とし、基地局が特定できる端末数(以下、特定端末数という)を1とし、前記各端末 i ($1 \leq i \leq N$)は、

$$S = \sum \lambda(i, \wedge) \times S_i \quad (\text{和は } i \in \wedge \text{について行う})$$

(ただし、

$$S_i = S + f_i \times i \bmod q \quad (f_i \text{は零でない } GF(q) \text{ の元})$$

$\lambda(i, \wedge) = \prod \{L / (L - i)\}$ (積は $L \in \wedge - \{i\}$ について行う)、

\wedge は、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報 S_i を秘密に保持しており、前記基地局は、前記 $(S, p, g, S_1, \dots, S_N)$ を保持し、

(1) 前記基地局は、 $GF(p)$ の元 g とし、零でない $GF(q)$ の元 k とし、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2) 前記基地局は、特定端末 a の秘密情報

S_aから排除情報

$$C_2 = g^k (k \times S_a \bmod q) \bmod p$$

を計算し、特定端末番号aと準備情報C₁と共に全端末に同報通信し、(3) 前記基地局は、前記特定端末aを除く全ての端末j(j ≠ a)との共有鍵

$$K = g^k (k \times S_j \bmod q) \bmod p$$

を求め、(4) 前記各端末j(j ≠ a)は、前記準備情報C₁と前記排除情報C₂と自身の秘密情報S_jを用いて、前記S_jと前記{j, λ}の前記法q^λ上の積を指數とする、前記C₁のべき乗剰余値

$$C_1 \wedge (S_j \times \lambda (j, \lambda) \bmod q) \bmod p$$

と、前記法q^λ上での求めた前記λ(a, λ)を指數とする、前記C₂のべき乗剰余値

$$C_2 \wedge (\lambda (a, \lambda) \bmod q) \bmod p$$

との積

$$C_1 \wedge (S_j \times \lambda (j, \lambda) \bmod q) \times C_2 \wedge (\lambda (a, \lambda) \bmod q) \bmod p$$

を計算することにより、前記基地局との共有鍵Kを求め、(i) 前記基地局は、零でないGF(q)の元eを任意に生成し、前記eを全端末に同報通信し、(ii) 前記基地局は、新規元

$$g' = g^{1/e} \bmod p$$

を求め、前記元gと置き換え、(iii) 前記各端末i

は、新規秘密情報

$$S'_i = S_i \times e \bmod q$$

(このとき、(g')^{ei} mod p = (g)^{ei} mod pが成り立つ)を求める排他的鍵共有法であり、基地局からのeのみの配達により少ない通信量で安全に端末秘密鍵の更新を行うという作用を有する。

【0021】本発明の請求項2記載の発明は、相互に接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他の鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、GF(p)の元をgとし、議長端末(任意の端末があることが可能)が特定できる特定端末数を1とし、前記各端末i(1 ≤ i ≤ N)は、

$$S = \sum \lambda (i, \lambda) \times S_i \quad (\text{和は } i \in \Lambda \text{について行う})$$

(ただし、

$$S_i = S + f_{i-1} \times i \bmod q \quad (f_{i-1} \text{は零でないGF}(q)\text{の元})$$

λ(i, λ) = IT {L / (L - i)} (積はL ∈ λ - {i}について行う)、

λは、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持しており、システム管理者により管理された前記素数p、前記約数q、前記元gと、前記システム管理者により管理された全端末の公開鍵

$$y = g^s \bmod p$$

と、前記システム管理者により管理された公報情報

$y_1 = g^{s1} \bmod p, y_2 = g^{s2} \bmod p, \dots, y_N = g^{sN} \bmod p$ を利用でき、(1) 前記議長端末は、零でないGF(q)の元kを任意に生成し、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2) 前記議長端末は、特定端末aの公開情報S_aから排除情報

$$C_2 = y^{k^a} \bmod p$$

を計算し、特定端末番号aと準備情報C₁と共に全端末に同報通信し、(3) 前記議長端末は、共有鍵

$$K = y^{k^a} \bmod p$$

を求め、(4) 前記各端末j(j ≠ a)は、Δ = {j, a}として、Δ(j, λ)とΔ(a, λ)を求め、前記準備情報C₁と前記排除情報C₂と自身の秘密情報S_jを用いて、

$$C_1 \wedge (S_j \times \Delta(j, \lambda) \bmod q) \times C_2 \wedge (\Delta(a, \lambda) \bmod q) \bmod p$$

を計算することにより、前記議長端末との共有鍵Kを求め、(i) 前記システム管理者は、零でないGF(q)の元eを任意に生成し、前記eを全端末に同報通信し、

(ii) 前記システム管理者は、新規元

$$g' = g^{1/e} \bmod p$$

を求め、管理する前記元gと置き換え、(iii) 前記各端末iは、新規秘密情報

$$S'_i = S_i \times e \bmod q$$

(このとき、(g')^{ei} mod p = (g)^{ei} mod pが成り立つ)を求める排他的鍵共有法であり、システム管理者によるeのみの少ない通信量の端末秘密鍵の配達で公開鍵暗号の秘密鍵を安全高速に更新するという作用を有する。

【0022】本発明の請求項3記載の発明は、基地局と、前記基地局と接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他の鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、基地局が特定できる端末数(以下、特定端末数という)を1とし、前記各端末i(1 ≤ i ≤ N)は、

$$S = \sum \lambda (i, \lambda) \times S_i \quad (\text{和は } i \in \Lambda \text{について行う})$$

(ただし、

$$S_i = S + f_{i-1} \times i \bmod q \quad (f_{i-1} \text{は零でないGF}(q)\text{の元})$$

λ(i, λ) = IT {L / (L - i)} (積はi ∈ λ - {i}について行う)。

λは、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持しており、前記基地局は、前記(S, p, g, S₁, ..., S_N)を保持し、(1) 前記基地局は、GF(p)の元をgとし、零でないGF(q)の元kとしたとき、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2) 前記基地局は、特定端末aの秘密情報S_aから排除情報

$$C_2 = g^{\wedge} (k \times S_a \bmod q) \bmod p$$

を計算し、特定端末番号aと準備情報C₁と共に全端末に向報通信し、(3)前記基地局は、前記特定端末aを除く全ての端末j(j ≠ a)との共有鍵

$$K = g^{\wedge}(k \times S \bmod q) \bmod p$$

を求め、(4)前記各端末j(j ≠ a)は、前記準備情報C₁と前記排除情報C₂と自身の秘密情報S_jを用いて、前記S_jと前記λ(j, λ)の前記法q上での積を指數とする、前記C₁のべき乗余数

$$C_1^{\wedge}(S_j \times \lambda(j, \lambda) \bmod q) \bmod p$$

と、前記法q上で求めた前記λ(a, λ)を指數とする、前記C₂のべき乗余数

$$C_2^{\wedge}(\lambda(a, \lambda) \bmod q) \bmod p$$

との積

$$C_1^{\wedge}(S_j \times \lambda(j, \lambda) \bmod q) \times C_2^{\wedge}(\lambda(a, \lambda) \bmod q) \bmod p$$

を計算することにより、前記基地局との共有鍵Kを求め、(i)前記基地局は、零でないGF(q)の元eを任意に生成し、前記共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、(ii)前記基地局は、新規元

$$g' = g^{1/e \bmod q} \bmod p$$

を求め、前記元gと置き換え、(iii)前記各端末jは、前記暗号化eを前記共有鍵Kを用いて復号化し、新規秘密情報

$$S'_j = S_j \times e \bmod q$$

(このとき、(g')^{S'_j} mod p = (g)^{S'_j} mod pが成立)を求める排他的鍵共有法であり、基地局により秘密鍵を更新して排除端末を継続的に排除するという作用を有する。

【0023】本発明の請求項4記載の発明は、相互に接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、GF(p)の元をgとし、議長端末bが特定できる特定端末数を1とし、前記各端末i(1 ≤ i ≤ N)は、

$$S = \sum \lambda(i, \Lambda) \times S_i \quad (\text{和は } i \in \Lambda \text{について行う})$$

(ただし、

$$S_i = S + f_{i-1} \times i \bmod q \quad (f_{i-1} \text{は零でない } GF(q) \text{ の元})$$

$$\lambda(i, \Lambda) = \prod (L/(L-i)) \quad (\text{積は } L \in \Lambda - \{i\} \text{について行う})$$

Λは、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持しており、全端末の公開鍵

$$y = g^S \bmod p$$

と、公開情報

$$y_1 = g^{S_1} \bmod p, y_2 = g^{S_2} \bmod p, \dots, y_N = g^{S_N} \bmod p$$

を利用でき、(1)前記議長端末bは、零でないGF(q)の元kを任意に生成し、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2)前記議長端末bは、特定端末aの公開情報y_aから排除情報

$$C_2 = y_a^k \bmod p$$

を計算し、特定端末番号aと準備情報C₁と共に全端末に向報通信し、(3)前記議長端末bは、共有鍵

$$K = y^k \bmod p$$

を求め、(4)前記各端末j(j ≠ a)は、Λ = {j, a}として、λ(j, Λ)とλ(a, Λ)を求めて、前記準備情報C₁と前記排除情報C₂と自身の秘密情報S_jを用いて、

$$C_1^{\wedge}(S_j \times \lambda(j, \Lambda) \bmod q) \times C_2^{\wedge}(\lambda(a, \Lambda) \bmod q) \bmod p$$

を計算することにより、前記議長端末との共有鍵Kを求め、(i)前記議長端末bは、零でないGF(q)の元eを任意に生成し、前記共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、(ii)前記議長端末bは、新規元

$$g' = g^{1/e \bmod q} \bmod p$$

を求めて、前記元gと置き換え、(iii)前記各端末jは、前記暗号化eを前記共有鍵Kを用いて復号化し、新規秘密情報

$$S'_j = S_j \times e \bmod q$$

(このとき、(g')^{S'_j} mod p = (g)^{S'_j} mod pが成立)を求める排他的鍵共有法であり、議長端末bにより公開鍵方式の秘密鍵を更新して排除端末を継続的に排除するという作用を有する。

【0024】本発明の請求項5記載の発明は、相互に接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、GF(p)の元をgとし、議長端末bが特定できる特定端末数を1とし、前記各端末i(1 ≤ i ≤ N)は、

$$S = \sum \lambda(i, \Lambda) \times S_i \quad (\text{和は } i \in \Lambda \text{について行う})$$

(ただし、

$$S_i = S + f_{i-1} \times i \bmod q \quad (f_{i-1} \text{は零でない } GF(q) \text{ の元})$$

λ(i, Λ) = Π (L/(L-i)) (積はL ∈ Λ - {i}について行う)、

Λは、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持しており、前記議長端末bは、全端末の公開鍵

$$y = g^S \bmod p$$

と、公開情報

y₁ = g^{S_1} mod p, y₂ = g^{S_2} mod p, ..., y_N = g^{S_N} mod p

を利用でき、(1)前記議長端末bは、零でないGF(q)の元kを任意に生成し、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2)前記議長端末bは、特定端末aの公開情報y_aから排除情報

$$C_2 = y_a^k \bmod p$$

を計算し、特定端末番号 a と準備情報 C_1 と共に全端末に同報通信し、(3) 前記議長端末 b は、共有鍵

$$K = y^k \bmod p$$

を求める。(4) 前記各端末 j ($j \neq a, b$) は、 $\Delta = \{j, a\}$ として、 $\lambda(j, \Delta)$ と $\lambda(a, \Delta)$ を求め、前記準備情報 C_1 と前記排除情報 C_2 と自身の秘密情報 S_j を用いて、

$$C_1^{\wedge} (S_j \times \lambda(j, \Delta) \bmod q) \times C_2^{\wedge} (\lambda(a, \Delta) \bmod q) \bmod p$$

を計算することにより、共有鍵 K を求める排他的鍵共有法であり、端末のみからなるシステムにおいて固定的な議長端末のみに端末排除の権限を与えて、端末排除を可能とするという作用を有する。

【0025】本発明の請求項6記載の発明は、請求項5記載の排他的鍵共有法において、前記議長端末 b を除く全ての端末は、前記議長端末 b の公開情報

$$y_b = g^{kb} \bmod p$$

を利用でき、前記議長端末 b が、前記議長端末 b の秘密情報 S_b を用いて、全端末に配送する特定端末番号 a と準備情報 C_1 と排除情報 C_2 に、デジタル署名を付加し、前記各端末 j が、前記議長端末の公開情報 y_b を用いて、署名の検証を行うものであり、議長端末が配送する情報に署名して、議長端末の配送する情報を端末が検証して安全性を高めるという作用を有する。

【0026】本発明の請求項7記載の発明は、請求項3、4記載の排他的鍵共有法において、上記基地局または議長端末が、上記特定端末 a に対して、上記元 e を配達し、上記特定端末 a は、新規秘密情報

$$S_a' = S_a \times e \bmod q$$

(このとき、 $(g')^{\wedge} S_a' \bmod p = (g)^{\wedge} S_a \bmod p$ が成り立つ) を求めるものであり、特定端末 a に e を配達して秘密鍵を更新することで、排除した特定端末 a を復帰させるという作用を有する。

【0027】本発明の請求項8記載の発明は、請求項1～7記載の排他的鍵共有法において、前記乗法演算を、任意の有限体上の楕円曲線などの曲線上の加法演算に対応せるものであり、演算速度を高速化するという作用を有する。

【0028】以下、本発明の実施の形態について、図1～図13を参照しながら詳細に説明する。

【0029】(第1の実施の形態) 本発明の第1の実施の形態は、基地局と複数の端末からなる同報通信が可能な通信システムにおいて、基地局が、零でない $GF(q)$ の元 c を任意に生成して全端末に同報通信し、新規元 $g^c (= g^{1/e} \bmod p)$ を求めて、元 g と置き換える、各端末 i が、新規秘密情報 $S_i' (= S_i \times e \bmod q)$ を求める排他的鍵共有法である。

【0030】図1は、本発明の第1の実施の形態の排他的鍵共有法における通信システムの通常状態を示す図で

ある。図1において、7は基地局、1～6は、基地局の管理下にある端末である。同報通信網8は、無線などにより同報通信が可能な通信路である。図2は、本発明の第1の実施の形態の排他的鍵共有法における元 g の更新方法を示す図である。図3は、本発明の第1の実施の形態の排他的鍵共有法における秘密鍵更新方法を示す図である。

【0031】図1～図3を参照して、本発明の第1の実施の形態の排他的鍵共有法について説明する。図1に示すように、基地局7は、秘密鍵 S を作成して、秘密に保持する。秘密鍵 S より大きく、端末数6より大きな素数または素数のべき p を作成して、保持する。 $(p-1)$ の約数 q を1つ求めて保持する。 $GF(q)$ の0でない元 f を求めて保持する。

【0032】 $f(z) = S + f_1 \times z \bmod q$ を用いて、 $S_i = f(i)$ を計算することにより求めた秘密情報 S_i を、各端末 i ($1 \leq i \leq 6$) に暗号通信手段を用いて秘密に配送する。

【0033】6台の端末の任意の2台からなる集合を八としたとき、秘密情報 S_i は、

$$S = \sum_{i=1}^8 \lambda(i, \Delta) \times S_i \quad (\text{和は } i \in \Delta \text{ について行う})$$

$$\lambda(i, \Delta) = \prod_{L \in \Delta} (L / (L - i)) \quad (\text{積は } L \in \Delta - \{i\} \text{ について行う})$$

を満たす。ただし、集合 $\Delta - \{i\}$ は、集合 Δ から集合 $\{i\}$ を除いた集合である。たとえば、 $\Delta = \{1, 2\}$ とすると、

$$\lambda(1, \Delta) = \prod_{L \in \Delta} (L / (L - 1)) \quad (L \in \{2\})$$

$$= 2 / (2 - 1) = 2$$

$$\lambda(2, \Delta) = \prod_{L \in \Delta} (L / (L - 2)) \quad (L \in \{1\})$$

$$= 1 / (1 - 2) = -1$$

$$\sum_{i=1}^8 \lambda(i, \Delta) \times S_i \quad (i \in \Delta)$$

$$= \lambda(1, \Delta) \times S_1 + \lambda(2, \Delta) \times S_2$$

$$= 2 \times f(1) - f(2)$$

$$= 2 \cdot (S + f_1) - (S + 2 \cdot f_1)$$

$$= S$$

となる。

【0034】各端末1, …, 6は、秘密情報 S_i を記憶部に保持する。基地局7は、法 p 、 $GF(p)$ の元 g を記憶部に保持する。基地局7は、秘密情報 S_1, \dots, S_6 をそれぞれ指數とし、 p を法とし、 g を底とした公開情報 $y_1 (= g^{S_1} \bmod p)$ 、 $y_2 (= g^{S_2} \bmod p)$ 、…、 $y_6 (= g^{S_6} \bmod p)$ を計算して記憶部に保持する。基地局7は、全端末1, …, 6の秘密鍵 S を指數とし、 p を法とし、 g を底とする全端末の公開鍵 $y (= g^S \bmod p)$ を計算して記憶部に保持する。

【0035】端末5を排除する場合を説明する。基地局7は、 $GF(q)$ の0でない元 k を任意に生成し、 k を指數とし、 p を法とし、 g を底とする準備情報 $C_1 (= g^k \bmod p)$ を計算する。整数 k を指數、 p を法とし、基地局7が特定した端末5の公開情報 y_5 を底とする排除情報

$C_2 (= y_{5^k} \bmod p)$ を計算する。kを指數、pを法、全端末1, ..., 6の公開鍵yを底とする共有鍵K ($= y^k \bmod p = g^k (S \times k) \bmod p$) を求める。以上のC₁、C₂および特定端末番号を全端末に同報通信する。

【0036】端末5を除いた全ての端末1, ..., 4, 6で共有鍵を共有する場合の鍵共有フェーズを説明する。端末1では、自己の端末番号1と、受信した排除端末番号5から、 $\Delta = (1, 5)$ として、

$$\lambda(1, \Delta) = 5 / (5 - 1) = 5 / 4$$

$$\begin{aligned} C_1 &= (S_1 \times \lambda(1, \Delta) \bmod q) \times C_2 \times (\lambda(5, \Delta) \bmod q) \bmod p \\ &= g^k (S_1 \times \lambda(1, \Delta) \bmod q) \bmod p \\ &\times g^k ((k \times S_5 \times \lambda(5, \Delta) \bmod q) \bmod p \\ &= g^k ((k \times (S_1 \times \lambda(1, \Delta) + S_5 \times \lambda(5, \Delta) \bmod q)) \bmod p \\ &= g^k (k \times S \bmod q) \bmod p \\ &= K \end{aligned}$$

を求めるることによりKを得る。

【0037】以上の計算は、端末2~4, 6でも同様に行うことができ、結果として、端末1~4, 6で共通鍵Kを共有することができる。

【0038】一方、端末5においては、基地局7から同報通信された排除情報C₂ ($= y_{5^k} = g^k (k \times S_5) \bmod p$) と、保持している情報から計算可能なべき乗剰余値 ($= C_1^{5^k} \bmod p = g^k (k \times S_5) \bmod p$) が、同じであること、 $\Delta = \{5\}$ となって $\lambda(5, \Delta)$ が求められないことから、上記鍵共有フェーズでの共有鍵Kの算出ができない。

【0039】各端末は、

$$\begin{aligned} K &= g^k (S \times k) \bmod p, \\ C_1 &= g^k \bmod p, \\ y &= g^k \bmod p \end{aligned}$$

から秘密鍵Sを求めることができないため、各分割秘密情報S_iは再利用できる。このため、次の鍵共有からはセットアップを行う必要はない、準備フェーズと鍵共有フェーズを繰り返せばよい。

【0040】図2を参照して、基地局7が元gを更新する方法を説明する。基地局7は、零でないGF(q)の元e(乱数)を任意に生成し、eを全端末に同報通信する。基地局7は、新規元

$$g' = g^{1/e} \bmod p$$

を求め、元gと置き換える。

【0041】図3を参照して、端末が秘密鍵を更新する方法を説明する。各端末1は、新規秘密情報

$$S_{1'} = S_1 \times e \bmod q$$

を求めて保持する。このとき、

$$(g')^{5^k} \bmod p = (g)^{5^k} \bmod p$$

が成立立つ。

【0042】上記のように、本発明の第1の実施の形態では、排他的鍵共有法を、基地局が、零でないGF(q)の元eを任意に生成して全端末に同報通信し、新規元g^{1/e mod p}を求めて、元gと置き換え、各端末1

$$\lambda(5, \Delta) = 1 / (1 - 5) = -1 / 4$$

を計算する。準備情報C₁ ($= g^k \bmod p$) と、排除情報C₂ ($= y_{5^k} \bmod p$) を用いて、S₁と $\lambda(1, \Delta)$ を指數とし、C₁を底とするべき乗剰余値

$$C_1 \times (\lambda(1, \Delta) \bmod q) \bmod p$$

と、 $\lambda(5, \Delta)$ を指數とし、C₂を底とするべき乗剰余値

$$C_2 \times (\lambda(5, \Delta) \bmod q) \bmod p$$

との積

が、新規秘密情報S₁ $\times e \bmod q$ を求める構成としたので、少ない通信量と計算量で秘密鍵を更新できる。

【0043】(第2の実施の形態) 本発明の第2の実施の形態は、相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、システム管理者が、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、新規元g^{1/e mod p}を求めて、管理する元gと置き換え、各端末1が、新規秘密情報S₁ $\times e \bmod p$ を求める排他的鍵共有法である。

【0044】図4は、本発明の第2の実施の形態の排他的鍵共有法における通常状態を示す図である。図4において、システム管理者9は、通信システムにアクセス可能な信頼できる機関であり、公開鍵を作成して端末に提供する。図5は、本発明の第2の実施の形態の排他的鍵共有法における元gの更新方法を示す図である。図6は、本発明の第2の実施の形態の排他的鍵共有法における秘密鍵の更新方法を示す図である。

【0045】図4~図6を参照して、本発明の第2の実施の形態の排他的鍵共有法について説明する。図4に示すように、相互に接続された6台の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、Sおよび6より大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、GF(p)の元をgとし、議長端末(任意の端末がなることができる)が特定できる特定端末数を1とする。

【0046】各端末1 ($1 \leq i \leq 6$) は、

$$S = \sum \lambda(i, \Delta) \times S_1 \quad (\text{和は } i \in \Delta \text{ について行う})$$

(ただし、

$$S_1 = S + f_1 \times i \bmod q \quad (f_1 \text{ は零でない GF(q) の元})$$

$\lambda(i, \Delta) = \prod_{L \in \Delta} (L - i)$ (積は $L \in \Delta - \{i\}$ について行う)。

は、6台の端末の任意の2台からなる集合である)を満たす秘密情報S₁を秘密に保持する。システム管理者により管理された素数p、約数q、元gと、システム管

理者により管理された全端末の公開鍵

$$y = g^k \bmod p$$

と、システム管理者により管理された公開情報

$y_1 = g^{s1} \bmod p, y_2 = g^{s2} \bmod p, \dots, y_6 = g^{s6} \bmod p$
を公開簿に載せて公開するので、各端末はこれらを利用できる。

【0047】議長端末は、零でないGF(q)の元kを任意に生成し、準備情報

$$C_1 = g^k \bmod p$$

を計算し、特定端末aの公開情報 y_a から排除情報

$$C_2 = y_a^k \bmod p$$

を計算し、特定端末番号aと準備情報 C_1 と共に全端末に同報通信する。議長端末は、共有鍵

$$K = y^k \bmod p$$

を求める。

【0048】各端末j ($j \neq a$)は、 $\Lambda = \{j, a\}$ として、 $\lambda(j, \Lambda)$ と $\lambda(a, \Lambda)$ を求め、準備情報 C_1 と排除情報 C_2 と自身の秘密情報 S_j を用いて、
 $C_1 \wedge (S_j \times \lambda(j, \Lambda) \bmod q) \times C_2 \wedge (\lambda(a, \Lambda) \bmod q) \bmod p$
 を計算することにより、議長端末との共有鍵Kを求める。

【0049】図5を参照して、元gの更新方法を説明する。システム管理者10は、零でないGF(q)の元e (乱数)を任意に生成し、eを全端末に同報通信する。システム管理者は、新規元
 $g' = g^{1/e} \bmod p$

を求め、管理する元gと置き換える。

【0050】図6を参照して、秘密鍵の更新方法を説明する。各端末1は、新規秘密情報

$$S'_1 = S_1 \times e \bmod q$$

を求めて保持する。このとき、 $(g')^{s1} \bmod p = (g)^{s1} \bmod p$ が成立つ。

【0051】上記のように、本発明の第2の実施の形態では、排他的鍵共有法を、システム管理者が、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、新規元 $g^{1/e} \bmod p$ を求め、管理する元gと置き換え、各端末1が、新規秘密情報 $S_1 \times e \bmod q$ を求める構成としたので、少ない通信量と計算量で秘密鍵を更新できる。

【0052】(第3の実施の形態) 本発明の第3の実施の形態は、基地局と接続された6台の端末からなる同報通信が可能な通信システムにおいて、基地局で、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、新規元 $g^{1/e} \bmod p$ を求め、元gと置き換え、各端末1が、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報 $S_1 \times e \bmod q$ を求める排他的鍵共有法である。

【0053】図7は、本発明の第3の実施の形態の排他的鍵共有法を示す図である。図8は、本発明の第3の実

施の形態の乱数配送方法を示す図である。図9は、端末を継続して排除する方法を説明する図である。

【0054】図7～図9を参照して、本発明の第3の実施の形態の排他的鍵共有法について説明する。図7に示すように、基地局7と、基地局7と接続された6台の端末からなる同報通信が可能な通信システムにおいて、秘密鍵をSとし、Sおよび6より大きい素数または素数のべき数をpとし、(-1)の約数をqとし、基地局が特定できる端末数 (以下、特定端末数という) を1とする。

【0055】各端末i ($1 \leq i \leq 6$)は、
 $S = \sum \lambda(i, \Lambda) \times S_i$ (和はi ∈ Λについて行う)
 (ただし、
 $S_i = S + f_1 \times i \bmod q$ (f_1 は零でないGF(q)の元)、

$\lambda(i, \Lambda) = \prod_{L \in \Lambda} (L/(L-1))$ (積は $L \in \Lambda - \{i\}$ について行う)、

Λは、6台の端末の任意の2台からなる集合である) を満たす秘密情報 S_i を秘密に保持している。

【0056】基地局は、(S, p, g, S₁, ..., S₆)を保持している。GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$$C_1 = g^k \bmod p$$

を計算する。特定端末3の秘密情報 S_3 から排除情報

$$C_2 = g^{\wedge}(k \times S_3 \bmod q) \bmod p$$

を計算し、特定端末番号3と準備情報 C_1 と共に全端末に同報通信する。特定端末3を除く全ての端末j ($j \neq 3$)との共有鍵

$$K = g^{\wedge}(k \times S \bmod q) \bmod p$$

を求める。

【0057】各端末j ($j \neq 3$)は、準備情報 C_1 と排除情報 C_2 と自身の秘密情報 S_j を用いて、 S_j と $\lambda(j, \Lambda)$ の法q上での積を指値とする。 C_1 のべき乗剩余値

$$C_1 \wedge (S_j \times \lambda(j, \Lambda) \bmod p)$$

と、法q上での求めた $\lambda(j, \Lambda)$ を指値とする、 C_2 のべき乗剩余値

$$C_2 \wedge (\lambda(j, \Lambda) \bmod p)$$

との積

$$C_1 \wedge (S_j \times \lambda(j, \Lambda) \bmod q) \times C_2 \wedge (\lambda(j, \Lambda) \bmod p)$$

を計算することにより、基地局との共有鍵Kを求めて保持する。

【0058】図8を参照して、乱数eの配送方法を説明する。基地局7は、零でないGF(q)の元e (乱数)を任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信する。新規元
 $g' = g^{1/e} \bmod p$

を求め、元gと置き換える。

【0059】図9を参照して、継続排除の方法を説明する。各端末1は、暗号化eを共有鍵Kを用いて復号化

し、新規秘密情報

$$S_j' = S_j \times e \bmod q$$

を求めて保持する。このとき、 $(g')^{S_j'} \bmod p = (g)^{S_j} \bmod p$ が成立つ。

【0060】上記のように、本発明の第3の実施の形態では、排他的鍵共有法を、基地局で、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、新規元 $g^{1/e} \bmod p$ を求め、元gと置き換え、各端末jが、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報 $S_j \times e \bmod q$ を求める構成としたので、少ない通信量と計算量で秘密鍵を更新でき、継続して特定端末を排除できる。

【0061】(第4の実施の形態) 本発明の第4の実施の形態は、相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、議長端末が、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、新規元 $g^{1/e} \bmod p$ を求め、元gと置き換え、各端末jが、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報 $S_j \times e \bmod q$ を求める排他的鍵共有法である。

【0062】図10は、本発明の第4の実施の形態の排他的鍵共有法を示す図である。図11は、本発明の第4の実施の形態の乱数配送方法を示す図である。図12は、端末を継続して排除する方法を示す図である。

【0063】図10～図12を参照して、本発明の第4の実施の形態の排他的鍵共有法について説明する。図10に示すように、相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、秘密鍵をSとし、Sおよびより大きい素数または素数のべき数をpとし、 $(p-1)$ の約数をqとし、GF(p)の元をgとし、議長端末(任意の端末がなることができる。ここでは、端末6を議長端末とする)が特定できる特定端末数を1とする。

【0064】各端末i ($1 \leq i \leq 6$)は、

$$S_i = \sum \lambda(i, \Delta) \times S_i \quad (\text{和は } i = \Delta \text{ について行う})$$

(ただし、

$$S_i = S + f_1 \times i \bmod q \quad (f_1 \text{は零でない } GF(q) \text{ の元})$$

$$\lambda(i, \Delta) = \prod_{j=1}^{\Delta} (L/(L-i)) \quad (\text{積は } L = \Delta - \{i\} \text{ について行う})$$

八は、6台の端末の任意の2台からなる集合である)を満たす秘密情報 S_i を秘密に保持している。全端末の公開鍵

$$y = g^S \bmod p$$

と、公開情報

$$y_1 = g^{S_1} \bmod p, y_2 = g^{S_2} \bmod p, \dots, y_6 = g^{S_6} \bmod p$$

を公開簿に載せて公開するので、各端末はこれらを利用できる。

【0065】議長端末は、零でないGF(q)の元kを任意に生成し、準備情報

$$C_1 = g^k \bmod p$$

を計算する。議長端末は、特定端末3の公開情報 y_3 から排除情報

$$C_2 = y_3^{-k} \bmod p$$

を計算し、特定端末番号3と準備情報 C_1 と共に全端末に同報通信する。議長端末は、共有鍵

$$K = y^k \bmod p$$

を求める。

【0066】各端末j ($j \neq 3$)は、 $\Delta = \{j, 3\}$ として、 $\lambda(j, \Delta)$ と $\lambda(3, \Delta)$ を求め、準備情報 C_1 と排除情報 C_2 と自身の秘密情報 S_j を用いて、

$$C_1 \wedge (S_j \times \lambda(j, \Delta) \bmod q) \times C_2 \wedge (\lambda(3, \Delta) \bmod q) \bmod p$$

を計算をすることにより、議長端末との共有鍵Kを求めれる。

【0067】図11を参照して、乱数の配送方法を説明する。議長端末は、零でないGF(q)の元e(乱数)を任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信する。議長端末は、新規元

$$g' = g^{1/e} \bmod p$$

を求める。元gと置き換える。

【0068】図12を参照して、継続排除の方法を説明する。各端末jは、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報

$$S_j' = S_j \times e \bmod q$$

を求めて保持する。このとき、 $(g')^{S_j'} \bmod p = (g)^{S_j} \bmod p$ が成立立つ。

【0069】上記のように、本発明の第4の実施の形態では、排他的鍵共有法を、議長端末が、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、新規元 $g^{1/e} \bmod p$ を求める。元gと置き換え、各端末jが、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報 $S_j \times e \bmod q$ を求める構成としたので、少ない通信量と計算量で秘密鍵を更新でき、継続して特定端末を排除できる。

【0070】なお、継続排除した端末を復帰させたために、新たに秘密鍵と公開鍵のペアを作成する必要があり、以前の公開鍵が使用できないが、新たに秘密鍵と公開鍵のペアを作成することなく、継続排除した端末を復帰させることができる。そのためには、次のようにすればよい。

【0071】基地局または議長端末が、特定端末3に対して、元eを配送し、特定端末3は、新規秘密情報

$$S_3' = S_3 \times e \bmod q$$

(このとき、 $(g')^{S_3'} \bmod p = (g)^{S_3} \bmod p$ が成立立つ)

を求める。このようにして、秘密鍵と公開鍵のペアを作成しないで、以前の公開鍵をそのまま使用することができる。特定端末が複数あり、そのうちのいくつかのみ復帰させる場合には、復帰させたい端末のみに秘密

にeを配送すればよい。

【0072】(第5の実施の形態) 本発明の第5の実施の形態は、相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、議長端末が、零でないGF(q)の元kを任意に生成し、準備情報C₁を計算し、特定端末番号aの公開情報y_aから排除情報C₂を計算し、特定端末番号aと準備情報C₁と共に全端末に同報通信し、共有鍵Kを求め、各端末は準備情報C₁と排除情報C₂と自身の秘密情報S_jを用いて、共有鍵Kを求める併他の鍵共有法である。

【0073】図13は、本発明の第5の実施の形態の併他の鍵共有法を示す図である。図13を参照して、本発明の第5の実施の形態の鍵共有方法について説明する。相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、秘密鍵をSとし、Sおよびより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、GF(p)の元をgとし、議長端末2が特定できる特定端末数を1とする。

【0074】各端末i(i=1≤i≤6)は、
 $S = \sum_{j=1}^6 \lambda(i, \Delta) \times S_j$ (和はi∈Δについて行う)
 (ただし、
 $S_1 = S + f_1 \times i \bmod q$ (f_1 は零でないGF(q)の元)、
 $\lambda(i, \Delta) = \prod_{l \in \Delta} \{L/(L-i)\}$ (積は $L \in \Delta - \{i\}$ について行う)。

△は、6台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持している。議長端末2は、全端末の公開鍵

$y = g^k \bmod p$

と、公開情報

$y_1 = g^{s_1} \bmod p, y_2 = g^{s_2} \bmod p, \dots, y_6 = g^{s_6} \bmod p$ を公開簿に載せて公開するので、各端末はこれらを利用できる。

【0075】議長端末2は、零でないGF(q)の元kを任意に生成し、準備情報

$C_1 = g^k \bmod p$

を計算する。特定端末aの公開情報y_aから排除情報
 $C_2 = y_a^k \bmod p$

を計算し、特定端末番号aと準備情報C₁と共に全端末に同報通信する。共有鍵

$K = y^k \bmod p$

を求める。

【0076】各端末j(j≠a,b)は、 $\Delta = \{j, a\}$ として、 $\lambda(j, \Delta)$ と $\lambda(a, \Delta)$ を求め、準備情報C₁と排除情報C₂と自身の秘密情報S_jを用いて、

$C_1 \wedge (S_j \times \lambda(j, \Delta) \bmod q) \times C_2 \wedge (\lambda(a, \Delta) \bmod q) \bmod p$

を計算することにより、共有鍵Kを求める。

【0077】なお、議長端末を除く全ての端末が、議長端末の公開情報

$$y_b = g^{s_b} \bmod p$$

を利用できるようにし、議長端末が、議長端末の秘密情報S_bを用いて、全端末に配送する特定端末番号aと準備情報C₁と排除情報C₂に、ディジタル署名を付加することにより、各端末jが、議長端末の公開情報y_bを用いて、署名の検証を行うことができる。

【0078】上記のように、本発明の第5の実施の形態では、併他の鍵共有法を、議長端末が、零でないGF(q)の元kを任意に生成し、準備情報C₁を計算し、特定端末番号aと準備情報C₁と共に全端末に同報通信し、共有鍵Kを求める。各端末は準備情報C₁と排除情報C₂と自身の秘密情報S_jを用いて、共有鍵Kを求める構成としたので、議長端末を固定して特定端末を排除できる。

【0079】なお、基地局または議長端末が、特定端末aに対して、元eを配送し、特定端末aが、新規秘密情報

$$S'_a = S_a \times e \bmod q$$

(このとき、 $(g')^k \times S'_a \bmod p = (g)^k \times S_a \bmod p$ が成立り立つ)を求めるにより、排除した端末を復帰させることができる。

【0080】また、乗法演算を、任意の有限体上の楕円曲線などの曲線上の加法演算に対応させることで、高速に演算することができる。

【0081】

【発明の効果】以上説明したように、本発明では、基地局と、基地局と接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの併他の鍵共有法を、秘密鍵をSとし、Sおよびより大きい素数または素数のべき数をpとし、(p-1)の約数をqとし、基地局が特定できる端末数(以下、特定端末数といふ)を1とし、各端末i(i=1≤i≤N)は、
 $S = \sum_{j=1}^N \lambda(i, \Delta) \times S_j$ (和はi∈Δについて行う)

(ただし、
 $S_1 = S + f_1 \times i \bmod q$ (f_1 は零でないGF(q)の元)、
 $\lambda(i, \Delta) = \prod_{l \in \Delta} \{L/(L-i)\}$ (積は $L \in \Delta - \{i\}$ について行う))。

△は、N台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持しており、基地局は、
 $(S, p, g, S_1, \dots, S_N)$ を保持し、(1)基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとしましたとき、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2)基地局は、特定端末aの秘密情報S_aから排除情報

$$C_2 = g^{s_a} \bmod p$$

を計算し、特定端末番号aと準備情報C₁と共に全端末に同報通信し、(3)基地局は、特定端末aを除く全ての端末j(j≠a)との共有鍵

$$K = g^{\wedge}(k \times S \bmod q) \bmod p$$

を求め、(4) 各端末 j ($j \neq a$) は、準備情報 C_1 と排除情報 C_2 と自身の秘密情報 S_j を用いて、 $S_j \wedge \lambda(j, \Delta)$ の法 q 上での積を指數とする、 C_1 のべき乗剩余値 $C_1^{\wedge}(S_j \times \lambda(j, \Delta) \bmod q) \bmod p$

と、法 q 上で求めた $\lambda(a, \Delta)$ を指數とする、 C_2 のべき乗剩余値

$$C_2^{\wedge}(\lambda(a, \Delta) \bmod q) \bmod p$$

との積

$$C_1^{\wedge}(S_j \times \lambda(j, \Delta) \bmod q) \times C_2^{\wedge}(\lambda(a, \Delta) \bmod q) \bmod p$$

を計算することにより、基地局との共有鍵 K を求め、

(i) 基地局は、零でない $G F(q)$ の元 e を任意に生成し、 e を全端末に同報通信し、(ii) 基地局は、新規元 $g' = g^{1/e} \bmod p$

を求め、元 g と置き換え、(iii) 各端末 i は、新規秘密情報

$$S_i' = S_i \times e \bmod q$$

(このとき、 $(g')^{\wedge} S_i' \bmod p = (g)^{\wedge} S_i \bmod p$ が成立する) を求める構成としたので、基地局の通信量が e のみと少なく、システムパラメータ元 g 以外の公開情報が変更されないので、高速に秘密情報の更新ができるという効果が得られる。

【0082】また、相互に接続された N 台 (N は 2 以上の整数) の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i) システム管理者は、零でない $G F(p)$ の元 e を任意に生成し、 e を全端末に同報通信し、(ii) システム管理者は、新規元 $g' = g^{1/e} \bmod p$

を求め、管理する元 g と置き換え、(iii) 各端末 i は、新規秘密情報

$$S_i' = S_i \times e \bmod q$$

を求める構成としたので、システム管理者の通信量が e のみと少なく、システムパラメータ元 g 以外の公開情報が変更されないので、高速に秘密情報の更新ができるという効果が得られる。

【0083】また、基地局と、基地局と接続された N 台 (N は 2 以上の整数) の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i) 基地局は、零でない $G F(q)$ の元 e を任意に生成し、共有鍵 K を用いて暗号化した暗号化 e を全端末に同報通信し、

(ii) 基地局は、新規元

$$g' = g^{1/e} \bmod p$$

を求め、元 g と置き換え、(iii) 各端末 j は、暗号化 e を共有鍵 K を用いて復号化し、新規秘密情報

$$S_j' = S_j \times e \bmod q$$

を求める構成としたので、排他的鍵共有で共有した共有鍵を用いて配送した乱数を用いて端末の秘密情報を更新して、以降の排他的鍵共有で排除した端末が復帰できないようにできるという効果が得られる。

【0084】また、相互に接続された N 台 (N は 2 以上の整数) の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i) 議長端末は、零でない $G F(q)$ の元 e を任意に生成し、共有鍵 K を用いて暗号化した暗号化 e を全端末に同報通信し、(ii) 議長端末は、新規元

$$g' = g^{1/e} \bmod p$$

を求め、元 g と置き換え、(iii) 各端末 j は、暗号化 e を共有鍵 K を用いて復号化し、新規秘密情報

$$S_j' = S_j \times e \bmod q$$

を求める構成としたので、排他的鍵共有で共有した共有鍵を用いて配送した乱数を用いて端末の秘密情報を更新して、以降の排他的鍵共有で排除した端末が復帰できないようにできるという効果が得られる。

【0085】また、相互に接続された N 台 (N は 2 以上の整数) の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵 S をとし、 S より N より大きい素数または素数のべき数を p とし、 $(p-1)$ の約数 q とし、 $G F(p)$ の元を g とし、議長端末 b が特定できる特定端末数を 1 とし、各端末 i ($1 \leq i \leq N$) は、

$$S = \sum \lambda(i, \Delta) \times S_i \quad (\text{和は } i \in \Delta \text{ について行う})$$

(ただし、

$$S_i = S + f_i \times i \bmod q \quad (f_i \text{ は零でない } G F(q) \text{ の元})$$

$\lambda(i, \Delta) = \prod_{j \in \Delta} (L - (L - j))$ (積は $j \in \Delta - \{i\}$ について行う)。

Δ は、 N 台の端末の任意の 2 台からなる集合である) を満たす秘密情報 S_i を秘密に保持しており、議長端末 b は、全端末の公開鍵

$$y = g^b \bmod p$$

と、公開情報

$$y_1 = g^{\wedge} \bmod p, y_2 = g^{\wedge} \bmod p, \dots, y_N = g^{\wedge N} \bmod p$$

を利用でき、(1) 議長端末 b は、零でない $G F(q)$ の元 k を任意に生成し、準備情報

$$C_1 = g^k \bmod p$$

を計算し、(2) 議長端末 b は、特定端末 a の公開情報 y_a から排除情報

$$C_2 = y_a^{-1} \bmod p$$

を計算し、特定端末番号 a と準備情報 C_1 と共に全端末に同報通信し、(3) 議長端末 b は、共有鍵 $K = y^b \bmod p$

を求め、(4) 各端末 j ($j \neq a, b$) は、 $\Delta = \{j, a\}$ として、 $\lambda(j, \Delta)$ をと $\lambda(a, \Delta)$ を求め、準備情報 C_1 と排除情報 C_2 と自身の秘密情報 S_j を用いて、

$$C_1^{\wedge}(S_j \times \lambda(j, \Delta) \bmod q) \times C_2^{\wedge}(\lambda(a, \Delta) \bmod q) \bmod p$$

を計算することにより、共有鍵 K を求める構成としたので、議長端末以外の端末は他の端末の公開情報を保持する必要が無く、議長端末のみが他の端末の公開情報を

利用できるので他の端末は議長端末になれないという効果が得られる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態の鍵共有方法における通常状態を示す図、

【図2】第1の実施の形態の鍵共有方法における元gの更新方法を示す図、

【図3】第1の実施の形態の鍵共有方法において秘密鍵の更新方法を示す図、

【図4】本発明の第2の実施の形態の鍵共有方法における通常状態を示す図、

【図5】第2の実施の形態の鍵共有方法における元gの更新方法を示す図、

【図6】第2の実施の形態の鍵共有方法において秘密鍵の更新方法を示す図、

【図7】本発明の第3の実施の形態の鍵共有方法における端末3の排除状態を示す図、

【図8】第3の実施の形態の鍵共有方法における乱数配

送方法を示す図、

【図9】第3の実施の形態の鍵共有方法における端末の離脱排除の方法を示す図、

【図10】本発明の第4の実施の形態の鍵共有方法における端末3の排除状態を示す図、

【図11】第4の実施の形態の鍵共有方法における乱数配送方法を示す図、

【図12】第4の実施の形態の鍵共有方法における端末の離脱排除の方法を示す図、

【図13】本発明の第5の実施の形態の鍵共有方法における議長端末の固定方法を示す図である。

【符号の説明】

1～6 端末1～端末6

7 基地局

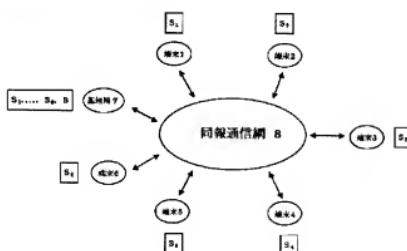
8 同報通信網

9 システム管理者

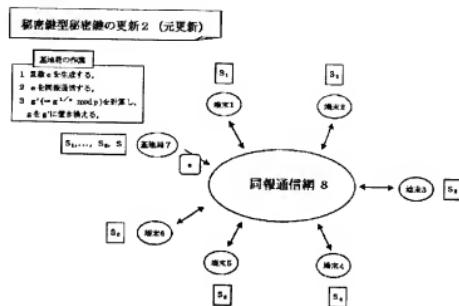
10 議長端末

【図1】

秘密鍵空密術鍵の更新1(通常状態)



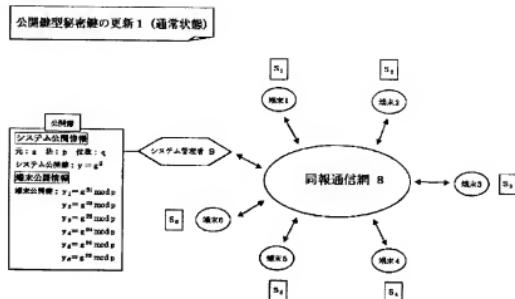
【図2】



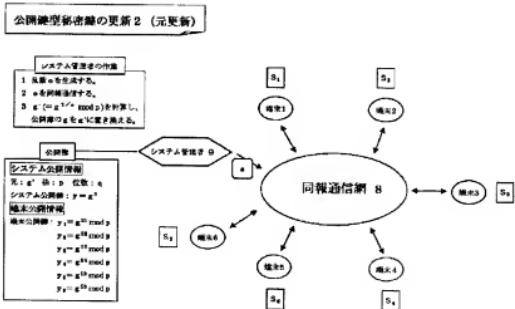
【図3】



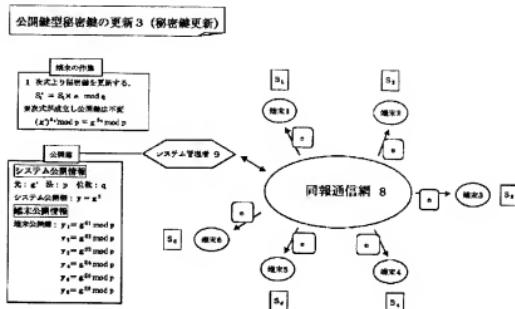
【図4】



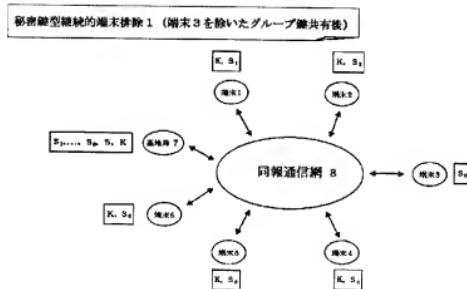
【図5】



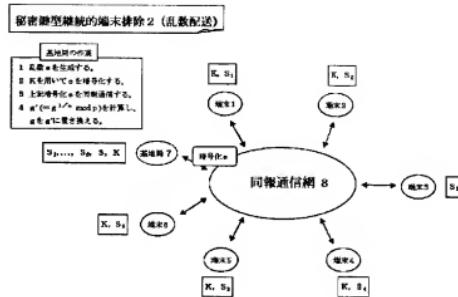
【図6】



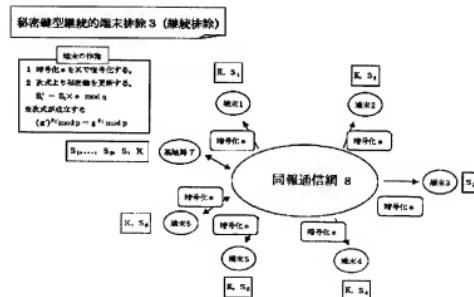
【図7】



【图8】

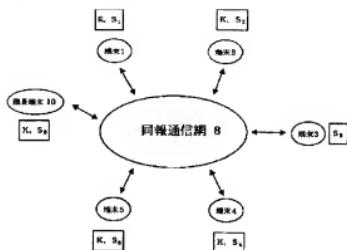


【图9】



【図10】

公開鍵型離散的端末排除1（端末3を除いたグループ鍵共有後）

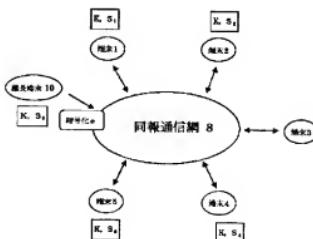


【図11】

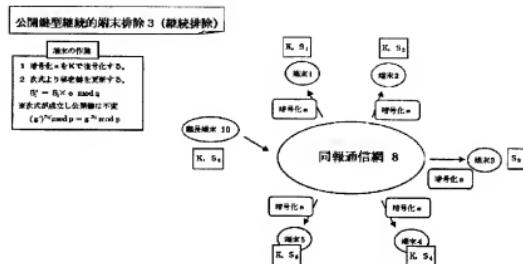
公開鍵型離散的端末排除2（混数配送）

端末選択の作業

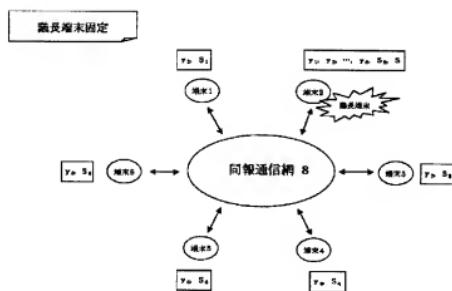
1. 端末を5台選定する。
2. Xを用いてeを標準化する。
3. 上記標準化eを各端末付ける。
4. e' (= e / (e - 1) * mod p) を計算し、
e'をeに書き換える。



【図12】



【図13】



フロントページの続き

(72)発明者 松崎 なつめ

神奈川県横浜市港北区新横浜三丁目20番地
8 株式会社高度移動通信セキュリティ技術研究所内

(72)発明者 松本 勉

神奈川県横浜市青葉区柿の木台13-45
F ターム(参考) 5J104 AA16 AA22 EA01 EA04 EA19
EA28 EA30 MA06 NA16 NA18
PA01 PA04 PA05
5K067 AA34 EE22 HH36